INFO-HAMS Digest Sat, 16 Dec 89 Volume 89 : Issue 1031

Today's Topics:

Date: 17 Dec 89 02:00:07 GMT
From: attctc!sampson@ames.arc.nasa.gov (Steve Sampson)
Subject: Cellular encryption
Message-ID: <10622@attctc.Dallas.TX.US>

In article <8912151446.AA23764@ti.com>, dube@cpdvax.csc.ti.com (DUBE TODD) writes:
>> "...even allows you to send messages to someone else who publishes his key..."
> Are you telling me that every person who has a phone can then communicate with
> ANYONE else who has a phone, safe in the knowledge that NO ONE else can decode
> and thus monitor his conversation?
> I'll eat my posting when you tell me how this is done, John.
>
> Regards,
> Dube Todd

You started this thread by being ignorant of crypto techniques and making the assumption that modern crypto hardware was easily broken into. What he was saying was that there are two keys. One you publish, the other you keep secret. The system is patented/copyright/trademarked (and God only knows what all) with the owners looking to make a billion before they die. I think they want to sell each package for the same price as a Chevy. What you are looking for is the Public-Key Cryptography. One key is used for encryption and made public, the other key is for decryption and kept secret. Personally I think something less complex would suffice. To answer your question, no.

Date: 16 Dec 89 21:14:45 GMT
From: cs.utexas.edu!natinst!rpp386!jeremy@tut.cis.ohio-state.edu (Jeremy S. Anderson)
Subject: Interception of E-Mail by spies
Message-ID: <17453@rpp386.cactus.org>

In article <7C`2N^@rpi.edu> joefritz@pawl.rpi.edu (Jochen M. Fritz) writes:

** I was just told by a friend that the
** government moniters and intercepts E-Mail
** messages that may contain information that may be
** detremential to "National Security".

Which agencies are responsible for this? Don't they also monitor long-distance phone conversations, international mail, etc? How much does this "service" cost the taxpayer?

Incidentally, what is the constitutional basis for the "National Security" justification that seems to outweigh all other considerations? Which agencies of the government have the right to classify different information as secret and which have the right to review these decisions?

As was mentioned in an earlier article, this power comes from a 1947(?) Executive order. This order, to my understanding is still kept at a very high level of secrecy.

(background information time: It is my understanding that the groups which review the confidentiality level of documents, do not posess the highest level of security clearance avalible. The outcome of this is amusing: there are documents which are classified at a higher level of security than the clearance groups can access. They have little choice but to renew the security level again and again...)

Monitoring of mail (and news) is not news. When I was active in the hacker culture, the byword was "the walls have ears and the ears listen with Crays." Another piece of background data (grade a rumor) The telephone co. is required to keep copies of all calls made over the past five years for law enforcement assistance. This came from a career employee of Pacific Northwest Bell, though I'm not sure if I would swallow this hook, line and sinker. I have never heard of electronic mail being intercepted for any National Security related purpose. The FBI will occasionally detain your mail if you show up at too many political rallies and work for too many leftist groups. I have never heard of them monitoring e-mail however. All stories I have heard about non-investigative communication monitoring come back to the NSA. I have known only one person that has had the NSA intervene with his activities. They tend not to be subtle.

** I am at a
** top technical school that has major ties to
** government money, so they have an excuse to
** censor *PRIVATE* messages between people. I was
** told of a person who wrote a message which
** contained numberous buzzwords, that would be
** found if any spies were looking. This message

```
**      was littered with phrases such as "pentagon",
**      "blow it up", "Laser tag", "Star Wars".  The
**      phrases were used completely out of military
**      context (ie we went to see "Star Wars")  The
**      message never made it through, and no record was
**      even kept of this message.

Sounds like an urban legend to me.
Or a faulty mailer...
**
**             This seems to be a gross infringement of
**      our constitutional right to freedom from
**      unreasonable search and seizure.  If anyone else
**      has any info on this, either post it or mail me
**      (I'll trust THEM)

Exactly what are one's rights when communicating over
computer networks? How do they compare to those regulating
intercepts of phone and mail communication?

The only reasonably secure means of E-mail transmission, if
you don't want someone somewhere to read it is encryption.
Therefore I was wondering if it is actually legal to mail
encrypted messages. Does it depend on whether the encryption
scheme is breakable by the government?  Does it matter whether
the communication is "in-house" or over "public utilities"?
(I don't know the correct terminology.) Is transmission of
encrypted messages over radio frequencies legal? Is the
transmission of encrypted messages over E-mail sufficient
legal grounds to open an investigation?

     E-mail privacy rights (and the right against your data transmissions
being tapped) are very shaky legal ground.  It is legal to mail encrypted
messages.  The crypt(1) function under UNIX is a childishly easy cipher to
break with the proper tools.  The crypt(3) library routine uses DES, which is
a little more sophisticated.  This cipher was developed by the NSA.  I
don't personally know how to break it, nor does anyone I have asked about it.
With sufficient brute-force application (i.e. 6 or 7 Cray-hours) I understand
it is breakable.  There is a rumor that combining these two encryption
methods carefully will produce a very strong cipher.  Perhaps an unbreakable
one.  This is a difficult area to provide hard facts on.  Most serious
professional cryptographers are either in corporate think-tanks or are with
the NSA.  Both groups usually have very heavy secrecy agreements over their
heads, which makes it difficult for me to locate qualified people to quiz
on this subject.

     The most important thing to take into account about the NSA is that
they are a monitoring agency.  They have no powers of prosecution by themselves
```

and the number of people who have access to their information banks are quite small. To answer an earlier dogging question: yes, this is an on your fourth ammendment rights of protection from unreasonable search and siezure. The draft is a violation of the fifteenth ammendment. The latter argument was heard in the Supreme court, agreed to be valid, and overridden on the grounds of -- national security. Are there any further questions??

JsA

--
There are two major products of Berkley, CA -- LSD and UNIX. We don't belive this to be strictly by coincidence.
Jeremy S. Anderson jeremy@rpp386.cactus.org LostIn, TX

Date: Sat, 16 Dec 89 13:22 PST
From: Chris Thomas <CSMSCST@OAC.UCLA.EDU>
Subject: Licence Turnaround Time

I have been waiting 56 days for my upgraded ticket (a->e + new call), and have recently begun wondering what's normal and when I should start getting worried. From scanning the Aug and Sept new extra calls in district 6, it seems that the FCC may be processing them as infrequently as once/month. Earlier this year, I submitted an address change, and got it back in about 32 days. Seeing as the VEC does all the work for upgrades, it wouldn't seem that there was much difference in the FCC processing required.

When I finally do get worried, does anyone have any suggestions whom to call? The FCC? The VEC? David Horowitz...

/Chris Thomas - WA6HTJ (AA6S-something?)

Internet: csmscst@oac.ucla.edu
Bitnet: csmscst@uclamvs.bitnet

Date: 16 Dec 89 21:00:57 GMT
From: tank!cps3xx!usenet@handies.ucar.edu (Usenet file owner)
Subject: Modifying Radios for out of band use
Message-ID: <5817@cps3xx.UUCP>

In article <102452@ti-csl.csc.ti.com> hoenig@tilde.UUCP (Mike Hoenig) writes:
> I was pointing out that I have modified my TH-75A by removing one

>   green wire behind the front case of the radio. This mod allows
>   full coverage of the 420-450MHz band, and then some. The display
>   will read out from 147.000 to 511.995. If anyone out there knows
>   how to tune the PLL, I'd appreciate that information. I'd like to
>   see if the rig will operate in the 220MHz band.
>
>   Also, I have modified my XYL's TH-25A, thanks to the posting of
>   those instructions here. I haven't yet tuned the PLL, but that's
>   "in the queue."
>
>   Mike (N5LTL; that's "Need 5 Ladies To Love")

I was the person who investigated and posted the mods for the th-x5at
Kenwood HTs (except the th-75at). You will not be able to retune the
pll in the radios as far as you are suggesting without extensive
modification to the pll. You would also need to do extensive
modification to other sections in the radio, namely all the RF sections.
I don't advise trying this; it's probably a lot cheaper and far less
frustrating to just go buy a radio already on a frequency close to the
one you are interested in.

Can you please post the info on how to modify the th-75at? I missed it
here. Thanks.

In the rare case that original ideas   Kenneth J. Hendrickson   N8DGN
are found here, I am responsible.   Owen W328, E. Lansing, MI 48825
Internet: kjh@usc.edu   UUCP: ...!uunet!usc!pollux!kjh

Date: 17 Dec 89 02:11:34 GMT
From: attctc!sampson@tut.cis.ohio-state.edu (Steve Sampson)
Subject: Packet compression
Message-ID: <10623@attctc.Dallas.TX.US>

In article <8912151531.AA24134@ti.com>, dube@cpdvax.csc.ti.com (DUBE TODD) writes:
> Marc Kaufman responds to Jim Grubbs' concern about compression: "However,
> I, for one, am getting tired of hearing from yhou why things can't be done.
> Why don't you just shut up and let us take our lumps (if any) from the FCC."
> Marc, are you saying that Hams should cease to be self-policing and just
> hand the burden to the FCC? I believe that every Ham should be concerned about
> the use of any methods or techniques that might work against the best interests
> of the hobby. And I DON'T think we should try to palm off the responsibility
> to the "Big Brother" we are all so afraid of. If the compression technique
> works within the established rules, then there's no problem; if not, then Jim
> has every reason to be concerned, as do the rest of us.
>
> Regards,

> Dube Todd, N5PDK

Unspecified codes can be used only in VHF and up. I'm thinking off the top of my head, but 2 meters and up come to mind. Jim Grubbs has never read the FCC rule book. I say that because everything he says is wrong. If not wrong, it's only because he reads the rules as a Communist would. Each community has a person of this type. They listen to the most active frequency and then tell us the rules. My reply is to have them notify the FCC, cause I ain't changing my operation on some stupid interpretation by an idiot. Self policing is more of a peer pressure than "on the air lawyers".

Steve, N5OWK

Date: 16 Dec 89 22:41:37 GMT
From: wshb!mikebat!michaelb@uunet.uu.net (Michael R. Batchelor)
Subject: rec.radio.shortwave "invite"
Message-ID: <167@mikebat.UUCP>

> In article <8460@ttidca.TTI.COM>, sorgatz@ttidca.TTI.COM (Avatar) writes...
>   (mindless drivel on swl'ers being dweebs and anti-Ham)
>
>   Hey Avatar, how are we gonna kiss your ass if you keep talking through
>   it? Sheesh, who are you anyway, The Incredible Iron Ham Man?

I agree. The guy has definatly lost it. If I wanted to have a fight I can go to any local bar and start one within a few minutes. That's a lot cheaper than either ham radio or computers.

When I was a kid I used to think hams were a wonderful bunch. I got excited about it and actually saved enough money to by Realistic DX-150. Then I got stopped cold by code. (Who does a 12 year old kid that lives in the boonies pratice with?) In later years I got interested again and found someone to work with me. With a little encouragement I actually got a liscense. Then I found the bands full of this kind of stuff and am now thoroughly disinterested in HF. I for one would fully support taking all HF bands away from the hams just to see if maybe we could get rid of some of the riff-raff.

Avatar, the signature is for you.

--
Michael Batchelor ..-. ..- -.-. -.-   -.-. --- -.. .   KA7ZNZ
uunet!wshb!mikebat!michaelb
I own this machine. It agrees with everything I say.

Date: 17 Dec 89 02:00:40 GMT
From: unmvax!ariel!hydra.unm.edu!ollie@ucbvax.Berkeley.EDU (David Oliver Eisman)
Subject: Wanted: rotors
Message-ID: <1134@ariel.unm.edu>

The Univ. of New Mexico Chapter of Students for the Exploration and
Development of Space (SEDS) is in need of some antenna rotors.

Student members of SEDS have been working on a permanent satellite
tracking facility known as the SEDS Satellite Tracking Station (SSTS).
The SSTS will be used to monitor transmissions from a variety
of spacecraft and satellites for educational purposes.
We also hope to use this groundstation for telecommand of our
own satellite, SEDSAT, to be launched in the next few years. Now, as many
members are studying for ham licenses and finishing up the radio-end
of the facility, it has become necessary to finish the antenna system.

We are looking for any working or repairable rotors that can be used
for satellite work. Right now we have a pair of KLM antennas that
could really use an az/el pair.

Thanks for the bandwidth.

73,

Ollie

If anyone on the net is willing to help us out with a donation of
a rotor or two, we'd really appreciate it.

Ollie Eisman - N6LTJ ollie@hydra.unm.edu
3505 Lafayette Rd. NE #3, Albuq, NM 87107
(505) 277-4845   or   (505) 884-7848

Date: 17 Dec 89 04:23:37 GMT
From: cs.utexas.edu!usc!zaphod.mps.ohio-state.edu!rpi!image.soe.clarkson.edu!
news@tut.cis.ohio-state.edu (Russ Nelson)
Subject: Weather FAX reciever for Radio Shack CoCo [rec.ham-
radio,rec.radio.shortwave]
Message-ID: <NELSON.89Dec16232332@image.clarkson.edu>

Are weather FAXes available for anonymous FTP?
--
--russ (nelson@clutx [.bitnet | .clarkson.edu])
Live up to the light thou hast, and more will be granted thee.
A recession now appears more than 2 years away -- John D. Mathon, 4 Oct 1989.

I think killing is value-neutral in and of itself. -- Gary Strand, 8 Nov 1989.
Liberals run this country, by and large. -- Clayton Cramer, 20 Nov 1989.
Shut up and mind your Canadian business, you meddlesome foreigner. -- TK, 23 N.

End of INFO-HAMS Digest V89 Issue #1031
****